动静态特征结合的漏洞风险评估及缓解方法 *

叶子维，郭渊博，琚安康

(信息工程大学，郑州 450000)

摘　要：针对如何提高漏洞风险评估的准确性进行了研究，提出一种动静态特征结合的漏洞风险评估及缓解方法。通过将传统风险评估方法中常用的来源于 CVSS 评分系统的攻击复杂度、影响程度、攻击向量等固定属性作为静态特征，将防御能力、漏洞修复情况、攻击者的攻击能力等随时间推移可能发生变化的属性作为动态特征，二者结合对漏洞的风险程度进行更加全面的评估。给出了在实际应用中各特征的量化计算方法，以及漏洞修复策略的推荐方法。以单个漏洞的风险评估过程和多个漏洞的风险评估结果为例，将评估结果与 CVSS 评分进行对比实验。结果表明该方法能结合具体的网络环境给出更加准确的漏洞风险评估结果及合理的漏洞修复策略，验证了该方法的可行性和有效性。

关键词：漏洞；风险评估；静态特征；动态特征

中图分类号：TP309.2　　doi: 10.19734/j.issn.1001-3695.2018.10.0759

Vulnerability risk assessment and mitigation method combining dynamic and static features

Ye Ziwei, Guo Yuanbo, Ju Ankang

(*Information Engineering University*, *Zhengzhou* 450000, *China*)

Abstract: Aiming at improving the accuracy of vulnerability risk assessment, this paper proposed a vulnerability risk assessment and mitigation method combining dynamic and static features. The method took fixed features such as attack complexity, impact degree and attack vector, which were commonly used in traditional risk assessment methods, as static features. And features such as defense capability, vulnerability repair and attacker's attack capability that may changed over time as dynamic features. The method combined the two kinds of features to make a more comprehensive assessment of the risk of vulnerabilities. Then this paper gave quantitative calculation method of each feature in practice and the recommendation method of vulnerability repair strategy. To verify the method, it took the risk assessment process of single vulnerability and the risk assessment results of multiple vulnerabilities as examples, and compared the results with CVSS scores. The experimental results show that the method can provide more accurate vulnerability risk assessment results and reasonable vulnerability repair strategy in combination with specific network environment, thus demonstrates the feasibility and effectiveness of the method.

Key words: vulnerability; risk assessment; dynamic feature; static feature

0　引言

随着传统互联网和工业控制网、物联网、移动互联网等特种网络技术的发展，网络安全问题的严重性正日益加剧。基于漏洞利用的网络攻击行为对各类网络系统的安全性造成了极大的威胁，因此研究漏洞的成因、归纳漏洞的类型、评估漏洞的风险程度，对于提高网络的抗攻击能力和自我修复能力具有重要意义。

目前在漏洞风险评估的理论研究方面，Fu 等人[1]提出一种基于粗糙集理论的漏洞风险程度评估方法，降低了在选择可能对漏洞风险程度造成影响的属性时对专家经验的依赖程度。唐成华等人[2]提出一种遗传模糊层次分析法，通过建立模糊判断矩阵和计算非线性优化问题的最优解求得软件漏洞的风险值。Huang 等人[3]基于 FAHP 算法，整合多种常用漏洞属性构建了安全漏洞评估框架，可满足多种场景下的漏洞风险评估需求。此外，部分研究人员还将现有方法应用到了移动互联网[4]、电信通信设备[5]、电力控制工业系统[6,7]等网络中。

通过总结现有研究成果可以看出，目前针对漏洞风险评估的研究，主要依据的仍是对漏洞自身属性的先验知识。而在具体的网络环境中，漏洞可修复性、现有防护措施、攻击者的攻击能力等随时可能发生动态变化的属性会对漏洞的实际风险程度产生影响，例如对于官方已提供修复方案的漏洞可通过安装官方补丁消除漏洞风险；通过部署针对具体攻击方式的防护措施可降低特定类型漏洞的风险程度；潜在攻击者的攻击能力越强，漏洞的风险越大。现有研究由于不能结合这些动态特征对漏洞的风险程度进行更精确地评估，会导致网络管理者对网络安全性及漏洞修复优先级产生误判。

针对以上问题，本文提出一种动静态特征结合的漏洞风险评估及缓解方法，将漏洞攻击复杂度、利用后果、利用向量（本地/邻近/远程）作为静态特征，将补丁状态、现有防护措施、攻击能力等作为动态特征，二者结合共同用于评估目标网络中各漏洞的风险程度，并根据风险程度评估结果对漏洞修复的优先级进行排序。

本文主要贡献如下：a）对漏洞的动静态特征进行分析和选取；b）提出一种动静态特征结合的漏洞风险评估方法，为

收稿日期：2018-10-05；**修回日期：**2018-11-21　　**基金项目：**国家自然科学基金资助项目（61602515，61501515）

作者简介：叶子维（1990-），男，博士研究生，主要研究方向为网络安全、态势感知（yezw2014@163.com）；郭渊博（1975-），男，教授、博导，主要研究方向为大数据安全、态势感知；琚安康（1995-），男，博士研究生，主要研究方向为网络攻击检测、威胁情报.

目标网络采取更进一步的安全防护措施提供依据；c）提出基于漏洞风险评估结果及漏洞类型的漏洞修复策略推荐方法，为网络管理者修复漏洞提供依据；d）以实例分析验证了本文提出方法的实用性和有效性。

1 相关工作

1.1 CVSS 标准

漏洞风险评估的核心之一是风险相关特征的量化，量化方法的优劣直接关系到风险评估结果的准确度和适用性。由于漏洞广泛存在于各类应用场景下的各种软硬件中，因此不同的厂商和机构对于漏洞风险评估的侧重点不尽相同，这导致了目前并没有统一的、各类场景通用的漏洞风险评估标准。

CVSS 标准是目前所有漏洞风险评估标准中普遍适用性最好、使用最广泛的标准，得到了包括美国国家漏洞数据库 NVD、国家信息安全漏洞共享平台 CNVD 等漏洞数据库，以及赛门铁克 Symantec、甲骨文 Oracle 等众多厂商的支持。2015 年 8 月 CVSS 在 2.0 版本的基础上进行了部分指标和评价体系的更新，发布了 3.0 版本，是目前最新的版本。相对于 CVSS 2.0 版本，3.0 版本主要增加了对漏洞之间互相影响情况的分析，采用了更加细粒度的攻击难度相关指标，并能对同一组件上存在的多个漏洞之间的利用链进行分析。上述新特性使得 3.0 版本具有更好的客观性和兼容性。

目前已有较多研究成果对 CVSS 标准进行了讨论和改进。Allodi 和 Younis 等人[8,9]讨论了 CVSS 标准对于漏洞的模式化分类和评分是否能准确评估漏洞带来的安全风险。Johnson 等人[10]讨论了在不同数据库和应用场景中 CVSS 标准是否具有普遍适用性。刘奇旭等人[20]研究了如何在 CVSS 标准的基础上进行更精细的漏洞安全等级划分。Ruohonen 等人[11]通过案例分析了漏洞从发现到收录的过程中的各种开销以及影响这些开销的要素。此外，部分学者研究了如何将 CVSS 标准应用于电信网络[12]、工业控制网络[13]等多种具体的应用场景中。

1.2 攻击能力分析

攻击者的能力高低直接影响了网络的风险程度。不同类型的目标网络通常会面对不同目的的潜在攻击者，而攻击者的攻击目的与攻击能力存在一定关联性，例如以满足政治诉求、获取经济利益的攻击者通常具有较高的攻击能力，而以测试自己技术水平、恶作剧为目的的攻击者通常攻击能力较低。对于不同能力的攻击者采取不同的防御措施，可以在满足安全需求的同时有效降低防御成本。

判断攻击者的能力高低，通常有两种方式。一种是在攻击发生前，根据己方网络的类型、存放数据的保密等级、攻击者可能的攻击目的等要素，预判潜在攻击者的攻击能力。在该研究方向上，Holsteijn[14]采用攻击树技术判断攻击者的攻击意图，从而判断攻击者的攻击能力，例如为了经济利益和为了技术挑战的攻击者对于攻击结果的评估是不同的，同时表现出的攻击能力也是不同的。Jaafor 等人[15]将社工攻击分为多个攻击阶段和攻击环境，以攻击者、被攻击者、发动攻击需要的资源（技术）、具体的攻击行为为元素，构建多层图模型，用于分析社交网站、论坛或博客中可能发生的社工攻击和潜在攻击者的攻击能力。Durkota 等人[16,17]通过将网络行为分解为自然行为（普通用户行为）、防御者行为和攻击者行为，假定攻击者可以获取当前网络状态，但无法预判防御者可能采取的防御措施，基于博弈论方法来评估攻击者可能的攻击能力和攻击行为。

另一种方式是在攻击发生时，根据攻击者采取的攻击方式、攻击强度、攻击目标等特征，判断当前攻击者的攻击能力。Fadlallah 等人[18]通过实验进行概念验证，证明了将攻击图技术和入侵检测技术结合可用于动态分析正在发动攻击的攻击者可能进行的后续攻击行为，从而判断攻击者的攻击目的和攻击能力。Pieters 等人[19]提出一种框架，在攻击过程中根据攻击者的投入实时判断攻击者的攻击能力和攻击强度，从而修正漏洞利用概率。

2 方法概述

本文提出的动静态特征结合的漏洞风险评估及缓解方法主要包含漏洞风险评估和漏洞修复策略推荐两个阶段。

2.1 漏洞风险评估

传统的基于 CVSS（common vulnerability scoring system，通用漏洞评分系统）标准的漏洞风险评估方法只考虑漏洞的攻击复杂度、攻击向量、影响程度等静态特征，导致大量漏洞的评分相同或相近，难以精确地体现出漏洞之间的差异性。且随着官方补丁的发布、攻击代码的公开、新防御能力的采用等条件变化，同一漏洞的风险程度也在发生变化。针对上述问题，本文提出一种动静态特征结合的漏洞风险评估方法，通过在传统方法的基础上结合动态特征对漏洞进行更加精细化的风险评估，来提供更加合理的漏洞修复策略。

2.1.1 面向风险评估的漏洞特征选取

如前文所述，本文将漏洞特征分为静态特征和动态特征两部分。其中，静态特征包含漏洞攻击复杂度、攻击向量和影响程度。在 CVSS 评分标准中，上述三个特征的取值如表 1 所示。其中攻击复杂度有三种取值，由低到高依次表示攻击复杂度的增加；攻击向量有三种取值，由低到高依次表示攻击者可以通过远程网络/需要从位于同一物理或逻辑网络中的主机上/只能从本机利用该漏洞发起攻击；影响程度表明该漏洞对受影响的组件在机密性、完整性、可用性方面的影响，通常在漏洞数据库中会给出量化值。

表 1 静态特征取值范围

Table 1 Value range of static features

特征	取值范围
攻击复杂度（attackcomplexity）	Low/medium/high
攻击向量（attackvector）	Network/adjacent/local
影响程度（impact）	(0,10]

动态特征包含防御能力、漏洞修复情况、攻击能力三部分。其中，防御能力特征表示当前网络中采用的防御措施对利用该漏洞发起的攻击的防御能力，表明网络自身对漏洞带来的风险的抵抗能力；漏洞修复情况特征表示软硬件厂商对自身产品中存在的漏洞发布官方补丁的情况，表明厂商对漏洞风险的缓解措施；攻击能力表示攻击者对利用该漏洞发动攻击的能力，表明攻击者的攻击技能对漏洞风险产生的影响。参考静态特征的取值范围，本文设定动态特征的取值范围如表 2 所示。

表 2 动态特征取值范围

Table 2 Value range of dynamic features

特征	取值范围
防御能力（defencecapbiliity）	[0,1]
漏洞修复情况（vulnerabilityrepair）	False/part/true
攻击能力（attackcapbility）	[0,1]

如表 2 所示，各特征取值范围说明如下：

a）防御能力取值为概率值，表示攻击者成功利用该漏洞发起攻击时网络对该攻击的防御概率。当取值为 0 时，表明当前网络中的防御机制不能发现或即使发现也无法阻止攻击；

当取值为 1 时，表示当前网络中的防御机制每次都能成功发现并阻止攻击。在实践中，该项特征可根据防御机制的历史记录，以漏洞类型为对象，统计针对基于特定类型的漏洞发起的攻击的防御成功率，作为该项特征的量化值。

b）漏洞修复情况取值分三类，由低到高依次表示目前尚无针对该漏洞的解决方案/官方未发布补丁但第三方安全机构发布了应急缓解方案/官方发布了可完全修复该漏洞的补丁。考虑到在实践中，可能存在如下情况：官方针对某一漏洞发布了补丁，但由于节点兼容性等原因，该补丁无法成功安装或安装后软硬件无法正常使用，或由于该补丁可能引入新漏洞等原因而主动放弃安装。此时应视为官方未发布针对该漏洞的补丁，取值根据实际情况取 False 或 Part。

c）攻击能力取值为概率值，表示攻击者利用该漏洞成功发动攻击的概率。当取值为 0 时，表示攻击者的能力不足以利用该漏洞发起攻击；当取值为 1 时，表示攻击者每次都可以成功利用该漏洞发起攻击。由于漏洞风险评估的主要应用是在攻击发生前指导如何修复网络漏洞和采取防护措施，因此此处对攻击者的攻击能力评估主要是根据网络特征预判潜在攻击者的攻击能力，而非在攻击发生时对攻击能力进行实时分析。目前已有学者研究了如何在实践中对攻击者的攻击能力进行评估，本文已在 1.2 节列举部分成果，此处不再赘述。

2.1.2 漏洞风险计算方法

参考文献[20]对静态特征中的攻击复杂度和攻击向量进行赋值，具体数值如表 3 所示。影响程度的量化值直接采用 NVD 给出的值。

表 3　静态特征量化值

Table 3　Quantization value of static features

特征	取值	量化值
攻击复杂度（attackcomplexity）	low	0.35
	medium	0.61
	high	0.71
攻击向量（attackvector）	network	1.0
	adjacent	0.65
	local	0.40
影响程度（impact）	slight	0.24
	part	0.63
	complete	1.0

动态特征取值中防御能力和攻击能力的取值已经是量化值。漏洞修复情况取值为 false/part/true，设对应量化值为 0/0.6/1。

在上述特征赋值基础上，提出漏洞风险评分公式，如下所示：

$$\text{RiskScore} = \lambda \times (\text{StaticScore} + \text{DynamicScore}) \tag{1}$$

公式中 *StaticScore* 和 *DynamicScore* 分别表示漏洞的静态特征和动态特征的综合评分,λ 为比例系数。其各自计算方式如下：

$$\text{StaticScore} = \text{AttackVector} \times \text{Impact} / \text{AttackComplexity} \tag{2}$$

$$\begin{aligned}\text{DynamicScore} = \ & (1 - \text{DefenceCapbiliity}) \times \\ & (1 - \text{VulnerabilityRepair}) \times \text{AttackCapbility}\end{aligned} \tag{3}$$

由特征取值范围可知，*StaticScore* 取值范围为 0.135~2.857，*DynamicScore* 取值范围为 0~1，因此综合漏洞风险评分 *RiskScore* 取值范围为 0.135~3.857。为将 *RiskScore* 取值范围调整至 0~10，使其上限与 CVSS 评分的取值范围上限相同，以符合一般使用习惯，计算得 λ=2.592，即

$$\text{RiskScore} = 2.592 \times (\text{StaticScore} + \text{DynamicScore}) \tag{4}$$

2.2　漏洞修复策略推荐

使用 2.1.2 节所述的漏洞风险计算方法对目标网络中的全部漏洞进行风险量化计算后，仍可能出现多个漏洞的风险评分相同或非常相近的情况。传统漏洞修复策略在这种情况下只能对这些漏洞给出相同的修复优先级，难以根据实际情况确定这些漏洞的修复顺序。针对这一缺陷，提出一种基于漏洞类型的漏洞风险比较方法，当多个漏洞风险评分相同时根据各自的漏洞类型确定修复优先级，最终给出细粒度的漏洞修复策略。该方法通过对不同类型漏洞的平均影响程度进行统计分析，对漏洞类型进行优先级排序。当有多个漏洞风险评分相同时，漏洞类型对应的平均影响程度较高的漏洞应当优先修复。该方法具体流程如下：

方法 1　基于漏洞类型的漏洞风险比较及修复策略推荐方法

a)统计一定时间段内 NVD 收录的漏洞的类型、数量和每个漏洞的影响程度评分；

b)对每种类型漏洞的平均影响程度进行计算；

c)根据平均影响程度对漏洞类型进行排序，排序结果用于对相同风险评分的漏洞进行修复优先级排序；

d)使用漏洞扫描器获取目标网络中的全部已知漏洞信息，设主机集合为 H，漏洞集合为 V；

e）计算每个漏洞的风险评分 RiskScore；

f)对全部漏洞根据风险评分由高到低进行排序，对于风险评分差值小于 0.5 的多个漏洞，根据漏洞类型的平均影响程度进行排序，若漏洞类型相同则作并列处理；

g)根据漏洞排序结果，输出漏洞修复策略。

上述步骤以算法表示如下：

算法 1 漏洞修复策略推荐算法

Input：NVD 收录的漏洞集合 V_{re}（包含漏洞类型 T 和漏洞影响 I），目标网络漏洞集合 V。

Output：漏洞修复策略 Seq(V)。

```
1  for (t=1;t≤n;t++)
2      i_t = (∑_{j=1}^{n_t} i) / n_t  ;
3  rank I_t;
4  for(s=1; s≤m; s++)
5    RiskScore(v_s);
6  rank RiskScore(V);
7  PRI(V)=count(RiskScore(V));
8  for(a=1; a≤m; a++)
9    for(b=a+1; b≤m)
10     if(|RiskScore(v_a)-RiskScore(v_b)|<0.5)
11       if(i_ta=i_tb)
12         set pri_a=pri_b;
13       else exchange(pri_a, pri_b);
14     end if
15   end for
16 end for
17 return Seq(V);
```

上述算法中，(1)~(3)行为根据漏洞类型计算平均影响程度并排序，其中 n 为漏洞类型集合 T 中的元素总数，即漏洞类型总数；i_t 为类型为 t 的全部漏洞的平均影响程度；n_t 为类型为 t 的漏洞的总数；I_t 为 i_t 的集合。(4)~(5)行为对目标网络中所有漏洞进行风险计算，其中 m 为漏洞集合 V 中的元素总数，即目标网络中已知漏洞的总数；v 为 V 中的元素。(6)行为对所有漏洞的风险评分进行排序，(7)为根据当前的风险评

分排序结果进行漏洞修复优先级排序。PRI(V)表示全部漏洞的修复优先级集合。(8)~(16)行为比较所有相邻的漏洞风险评分，若有评分差值小于 0.5 且不为 0 的两个漏洞，则将对应漏洞类型的平均影响程度较高的漏洞的修复优先级提前；若评分相同，则两个漏洞修复优先级相同。i_{ta} 和 i_{tb} 分别表示漏洞 a 和漏洞 b 对应的漏洞类型的平均影响程度；pri_a 和 pri_b 分别表示漏洞 a 和漏洞 b 的修复优先级。(17）行为根据最终的漏洞修复优先级排序结果输出漏洞修复策略 Seq(V)，即推荐的漏洞修复序列，顺位越靠前的漏洞越需要优先修复。

3　实验验证

3.1　单个漏洞风险评估案例

以漏洞 CVE-2018-14359 为例说明本文方法在实践中如何使用。

CVE-2018-14395 是一个存在于 Mutt 和 NeoMutt 的缓冲区溢出漏洞，通过利用该漏洞攻击者可以实现任意代码执行。从美国国家数据库 NVD 中获取该漏洞的部分信息如表 4 所示。

表 4　CVE-2018-14395 漏洞信息

Table 4 Information of CVE-2018-14395

参数	CVSS 2.0	CVSS 3.0
漏洞编号	CVE-2018-14359	CVE-2018-14359
攻击复杂度	10.0	3.9
攻击向量	network	network
影响程度	5.9	6.4
漏洞公开时间	2018.06.22	2018.06.22
补丁发布时间	2018.07.16	2018.07.16
CVSS 评分	7.5	9.8

由表 4 可知，CVSS 2.0 版本和 CVSS 3.0 版本对该漏洞的主要分歧点在于攻击复杂度和综合评分。CVSS 3.0 相对于 CVSS 2.0 大幅降低了该漏洞的攻击复杂度，略微提高了该漏洞的影响程度，攻击向量无变化，因此综合风险评分有较大幅度的提升。

假定在某目标网络中存在该漏洞，且尚无针对该漏洞的官方补丁或应急缓解方案，以该网络为攻击目标的攻击者每次都能利用该漏洞成功发起攻击。通过统计分析历史日志，得知该网络中采用的防护措施对基于该类型漏洞发起的攻击有 0.8 的防御成功概率。

1）CVSS 2.0

根据式(1)~(3)计算得到静态特征评分 *StaticScore*=0.63*1.0/0.71=0.887，动态特征评分 *DynamicScore*=(1-0.8)*(1-0)*1=0.2，综合漏洞风险评分 *RiskScore*=2.592*(0.887+0.2)=2.818。

2）CVSS 3.0

根据式(1)~(3)计算得到静态特征评分 *StaticScore*=0.63*1.0/0.35=1.800，动态特征评分 *DynamicScore*=(1-0.8)*(1-0)*1=0.2，综合漏洞风险评分 *RiskScore*=2.592*(1.800+0.2)=5.184。

将计算结果与 CVSS 给出的评分进行对比，当采用 CVSS 2.0 标准时，本文方法得出的漏洞风险评分为 2.818 分，小于 CVSS 给出的 7.5 分；当采用 CVSS 3.0 标准时，本文方法得出的漏洞风险评分为 5.184 分，小于 CVSS 给出的 9.8 分。由此可知尽管该漏洞是一个高危漏洞，但由于目标网络中采用的防护机制对基于该类型漏洞发起的攻击有较好的防御效果，因此无论是采用 2.0 标准还是 3.0 标准，该漏洞对于目标网络的风险程度都远低于 CVSS 给出的综合评分。

3.2　多个漏洞风险评估及修复策略推荐实验

为验证本文方法对网络中多个漏洞的评估结果和修复策略推荐的准确性和有效性，使用漏洞扫描工具 Nessus 对实验网络中某主机进行漏洞扫描，共发现 5 个漏洞，其静态特征信息如表 5 所示。

通过查询相关信息可知，CVE-1999-0499、CVE-1999-0517 和 CVE-2017-0267 三个漏洞被攻击者成功利用时会导致信息泄露；CVE-2016-0128 被攻击者成功利用时会导致目标主机受到中间人攻击；CVE-2017-0143 被攻击者成功利用时会导致任意代码执行。根据漏洞公开和补丁发布时间，假定 CVE-1999-0499、CVE-1999-0517 和 CVE-2016-0128 已有官方发布的可安装的修复补丁；CVE-2017-0143 的官方补丁由于兼容性问题无法安装，只能采用第三方安全公司提供的缓解方案；CVE-2017-0267 暂无官方或第三方解决法案。此外，假定攻击者每次都能利用上述漏洞都能成功发起攻击，网络中采用的防护机制对信息泄露攻击的防御概率为 0.8，对中间人攻击的防御概率为 0.5，对任意代码执行攻击的防御概率为 0.2。则采用本文方法，计算得到 5 个漏洞的综合风险评分如表 6 所示。

表 5　实验主机漏洞信息（基于 CVSS 2.0 标准）

Table 5　Vulnerabilities on experimental host (based on CVSS 2.0 standard)

参数	CVE-1999-0499	CVE-1999-0517	CVE-2016-0128	CVE-2017-0143	CVE-2017-0267
攻击复杂度	low	low	medium	medium	medium
攻击向量	network	network	network	network	network
影响程度	6.4	6.4	4.9	10.0	2.9
漏洞公开时间	1997.01.01	1997.01.01	2016.03.23	2017.03.14	2017.05.09
补丁发布时间	1999.06.07	1998.11.17	2016.04.12	2017.03.14	2017.05.09
CVSS 评分	7.5	7.5	5.8	9.3	4.3

表 6　漏洞风险评估结果（基于 CVSS 2.0 标准）

Table 6　Results of vulnerability risk assessment(based on CVSS 2.0 standard)

参数	CVE-1999-0499	CVE-1999-0517	CVE-2016-0128	CVE-2017-0143	CVE-2017-0267
StaticScore	1.829	1.829	0.803	1.639	0.475
DynamicScore	0	0	0	0.32	0.2
RiskScore	4.740	4.740	2.082	5.078	1.751

由上表中的风险评估结果可以看出，由于网络中采用了针对任意代码执行攻击的防护机制，尽管 CVE-2017-0143 漏洞在 CVSS 2.0 标准下评分高达 9.3 分，但在目标网络中风险程度较低，仅为 5.078 分；CVE-1999-0499 和 CVE-1999-0517 两个漏洞虽然利用后果是风险程度较低的信息泄露，但由于攻击复杂度低、影响程度较高，应当次优先修复，且由于漏洞类型相同，所以优先级相同；CVE-2016-0128 和 CVE-2017-0267 在目标网络中风险程度很低，可将修复次序放在最后。综上所述，最终推荐的漏洞修复策略为 CVE-2017-0143 > CVE-1999-0499 = CVE-1999-0517 >

CVE-2016-0128 > CVE-2017-0267.

此外，由于 CVE-1999-0499、CVE-1999-0517 没有 CVSS 3.0 评分，因此本文在表 7 和 8 中仅给出其他三个漏洞在 CVSS 3.0 标准下的漏洞信息和风险评估结果作为参考。

表 7　实验主机漏洞信息（基于 CVSS 3.0 标准）

Table 7　Vulnerabilities on experimental host(based on CVSS 3.0 standard)

参数	CVE-2016-0128	CVE-2017-0143	CVE-2017-0267
攻击复杂度	High	High	High
攻击向量	Network	Network	Network
影响程度	5.2	5.9	3.6
漏洞公开时间	2016.03.23	2017.03.14	2017.05.09
补丁发布时间	2016.04.12	2017.03.14	2017.05.09
CVSS 评分	6.8	8.1	5.9

表 8　漏洞风险评估结果（基于 CVSS 3.0 标准）

Table 8. Results of vulnerability risk assessment(based on CVSS 3.0 standard)

参数	CVE-2016-0128	CVE-2017-0143	CVE-2017-0267
StaticScore	0.732	0.831	0.507
DynamicScore	0	0.32	0.2
RiskScore	1.897	2.983	1.833

4　结束语

特定漏洞在具体网络中的风险程度随漏洞可修复性、现有防护机制、攻击能力等特征的变化而变化。考虑到这种变化趋势会直接影响网络管理者对修复漏洞、增加防护机制等安全防护行为的实施优先级，本文提出一种动静态特征结合的漏洞风险评估及缓解方法，通过将上述可变特征作为动态特征，将攻击复杂度、影响程度、攻击向量等相对稳定的特征作为静态特征，二者结合对漏洞的风险程度进行评估。评估结果用于分析网络整体安全性及具体漏洞对网络安全性的影响，并以此为依据进行漏洞修复策略的推荐，从而指导网络管理者对网络采取加固措施。

后续工作中将进一步研究是否还有其他尚未考虑到的动态特征，以及如何在本文方法中引入这些新特征以便进一步提高漏洞风险评估的准确性。

参考文献：

[1] Fu Zhiyao, Gao Ling, Sun Qian, *et al.* Evaluation of vulnerability severity based on rough sets and attributes reduction [J]. Journal of Computer Research and Development, 2016, 53 (5): 1009-1017.

[2] 唐成华，田吉龙，汤申生，等. 一种基于 GA-FAHP 的软件漏洞风险评估方法 [J]. 计算机科学, 2015, 42 (9): 134-138. (Tang Chenghua, Tian Jilong, Tang Shensheng, *et al.* Risk assessment of software vulnerability based on GA-FAHP [J]. Computer Science, 2015, 42 (9): 134-138.)

[3] Huang Chiencheng, Lin Fengyu, Lin Yeongsung, *et al.* A novel approach to evaluate software vulnerability prioritization [J]. Journal of Systems & Software, 2013, 86 (11): 2822-2840.

[4] Li Shancang, Tryfonas T, Russell G, *et al.* Risk assessment for mobile systems through a multilayered hierarchical Bayesian Network [J]. IEEE Trans on Cybernetics, 2016, 46 (8): 1749-1759.

[5] Wiik J, Gonzalez J J, Lipson H F, *et al.* Dynamics of vulnerability-modeling the life cycle of software vulnerabilities [C]// Proc of the 22th International System Dynamics Conference. 2004: 1-20.

[6] Ciapessoni E, Cirio D, Kjølle G, *et al.* Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties [J]. IEEE Trans on Smart Grid, 2016, 7 (6): 2890-2903.

[7] 杨国泰，王宇飞，罗剑波，等. 电力 CPS 信息网络脆弱性及其评估方法 [J]. 中国电力, 2018, 51 (1): 83-89. (Yang Guotai, Wang Yufei, Luo Jianbo, *et al.* Vulnerability of power CPS information network and its evaluation method [J]. Electric Power, 2018, 51 (1): 83-89.)

[8] Allodi L, Massacci F. Comparing vulnerability severity and exploits using case-control studies [J]. ACM Trans on Information & System Security, 2014, 17 (1): 1-20.

[9] Younis A, Malaiya Y K, Ray I. Evaluating CVSS base score using vulnerability rewards programs [C]//Proc of IFIP International Information Security and Privacy Conference. Switzerland: Springer International Publishing, 2016: 62-75.

[10] Johnson P, Lagerstrom R, Ekstedt M, *et al.* Can the common vulnerability scoring system be trusted?a Bayesian analysis [J]. IEEE Trans on Dependable & Secure Computing, 2016, PP (99): 1-1.

[11] Ruohonen J, Holvitie J, Hyrynsalmi S, *et al.* Exploring the clustering of software vulnerability disclosure notifications across software vendors [C]//Proc of the 13th IEEE/ACS International Conference of Computer Systems and Applications. Piscataway,NJ: IEEE Press, 2016: 1-8.

[12] 李伟. 漏洞量化评分方法在电信安全策略中的应用 [J]. 网络安全技术与应用, 2015, 2 (2): 27-28. (Li Wei. Application of vulnerability quantification scoring method in Telecom security strategy [J]. Network security technology and application, 2015, 2 (2): 27-28.)

[13] 王作广，魏强，刘雯雯. 基于攻击树与 CVSS 的工业控制系统风险量化评估 [J]. 计算机应用研究, 2016, 33 (12): 3785-3790. (Wang Zuoguang, Wei Qiang, Liu Wenwen. Quantitative risk assessment of industrial control systems based on attack-tree and CVSS [J]. Application Research of Computers, 2016, 33 (12): 3785-3790.)

[14] Rick V H. The motivation of attackers in attack tree analysis [D]. Delft, Holland: Delft University of Technology, 2015.

[15] Jaafor O, Birregah B. Multi-layered graph-based model for social engineering vulnerability assessment [C]//Proc of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. New York: ACM Press, 2016: 1480-1488.

[16] Durkota K, Lisý V, Bošanský B, *et al.* Approximate solutions for attack graph games with imperfect information [C]//Proc of International Conference on Decision and Game Theory for Security. Switzerland: Springer, 2015: 228-249.

[17] Durkota K, Lisy V, Kiekintveld C, *et al.* Case studies of network defense with attack graph games [J]. IEEE Intelligent Systems, 2016, 31 (5): 24-30.

[18] Fadlallah A, Sbeity H, Malli M, *et al.* Application of attack graphs in intrusion detection systems:an implementation [J]. International Journal of Computer Networks, 2016, 8 (1): 1-12.

[19] Pieters W, Davarynejad M. Calculating adversarial risk from attack trees: Control strength and probabilistic attackers [M]// Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Switzerland: Springer, 2015: 201-215.

[20] 刘奇旭，张翀斌，张玉清，等. 安全漏洞等级划分关键技术研究 [J]. 通信学报, 2012,33 (S1): 79-87. (Liu Qixu, Zhang Chongbin, Zhang Yuqing, *et al.* Research on key technology of vulnerability threat classification [J]. Journal on Communications, 2012,33 (S1): 79-87.)